UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/683,584	10/09/2003	Yung Chang Liang	TRNDP015	7721

22434 7590 07/18/2007

BEYER WEAVER LLP
P.O. BOX 70250
OAKLAND, CA 94612-0250

EXAMINER	
NGUYEN, KHOI	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
07/18/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/683,584	LIANG, YUNG CHANG	
	Examiner	Art Unit	
	Khoi Nguyen	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 1 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 April 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-18 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4)☒ Interview Summary (PTO-413) Paper No(s)/Mail Date. *20070601*.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. Applicant's amended claims 1-2, 6, and 10-18 and has been fully considered and is entered.

Response to Arguments

2. Applicant's arguments filed 04/17/2007 with respect to claims 1-18 have been fully considered but they are moot in view of the new ground(s) of rejection. The new grounds of rejection are necessitated by Applicant's amendment to the claims.

3. Applicant argued that "White does not describe creating an anti-virus agent where the detection module of the agent identifies client devices that have been affected by a virus as well as those that have not..... implemented via the payload, tailored to address the specific virus that originally affected the client device" (see page 6, 4th paragraph entirely) has been fully considered but they are not persuasive. It is true that the White reference does not disclose the construct of the actual virus packet to be used as a means to combat the real virus. However, White disclosed a distributed infrastructure where the actual virus was analyzed (copy the actual virus and forward to the virus analysis center for generating the cure) to generate a virus signature and the .dat file that is used

to remedy the actual virus and inoculate other clients that have not been infected yet (White, Fig. 3, and associated text on pages 10-15).

Furthermore, the Cass reference discloses the structure of the Melissa virus, which comprise a detection, an infection, and a payload module where the virus would detect to see if a client has been infected. If not, it infects the client and moves on to the next one ("Source of Mischief" section, page 59). It would have been obvious for one of the skill in the art to modify the White reference with the method taught by Cass to provide an effective defense by understanding the cause and mechanism of infection (Cass, page 56, paragraph 5, lines 1-3).

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claim 10 is rejected under 35 U.S.C. 102(b) as being anticipated by White et al. ("Anatomy of a Commercial-Grade Immune System, IBM Research White Paper, 1999, http://www.research.ibm.com/antivirus/SciPapers/White/Anatomy/Anatomy.PDF), hereafter "White".

6. With regard to claim 10, White discloses a distributed network having a number of server computers and associated client devices, computer readable medium for creating an anti-computer virus agent, comprising:

Computer code (section "download floods", page 8, line 4, anti-virus software reads on computer code) for parsing a selected computer virus (section "Immune System architectural overview" page 10, paragraph 1, lines 3-4, analyze a new or previously unknown virus reads on parsing a selected computer virus); and based upon the parsing (section "Virus Analysis" page 13, lines 1-3, use the result of this analysis reads on based upon the parsing).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-6 and 11-15 are rejected under 35 USC 103(a) as being unpatentable over White et al. ("Anatomy of a Commercial-Grade Immune System, IBM Research White Paper, 1999, http://www.research.ibm.com/antivirus/SciPapers/White/Anatomy/Anatomy.PDF), hereafter "White" and in view of Cass ("Anatomy of Malice", Spectrum IEEE, Nov. 2001, vol. 35, issue 11, pages: 56-60), hereafter "Cass".

9. With regard to claim 1, White discloses a distributed network having a number of server computers and associated client devices (Fig. 2), method of creating an anti-computer virus agent, comprising:

parsing a selected computer virus (section "Immune System architectural overview" page 10, paragraph 1, lines 3-4, analyze a new or previously unknown virus reads on parsing a selected computer virus); and based upon the parsing (section "Virus Analysis" page 13, lines 1-3, use the result of this analysis reads on based upon the parsing).

modifying the parsed virus (section "Virus Analysis", page 13, lines 1-3, create a test and cure for the new virus reads on modifying the parsed virus) to repair those client devices infected by the selected virus (section "Cure Distribution", page 13, lines 1-4)

However, White does not disclose a detection module for detecting whether a client device is presently infected with a virus, triggers the introduction of an anti-virus infection module so that the virus in a client device is overwritten, wherein an anti-virus agent payload, created based on features of the selected computer virus, performs as a cleaning/repairing payload capable of cleaning and repairing damage done to the client device, the payload also capable of inoculating the

client device against the virus in cases where the client device was not infected by the computer virus.

Cass, on the hand, discloses a detection module for detecting whether a client device is presently infected with a virus, triggers the introduction of an anti-virus infection module so that the virus in a client device is overwritten, wherein an anti-virus agent payload, created based on features of the selected computer virus, performs as a cleaning/repairing payload capable of cleaning and repairing damage done to the client device, the payload also capable of inoculating the client device against the virus in cases where the client device was not infected by the computer virus ("Source of Mischief" section, page 59).

It would have been obvious for one of the skill in the art to modify the White reference with the method taught by Cass to provide an effective defense by understanding the cause and mechanism of infection (Cass, page 56, paragraph 5, lines 1-3).

10. With regard to claims 2 and 11, White discloses a method and a computer readable medium for virus analysis (abstract) but does not disclose the selected computer virus is formed of a detection module, an infection module, and a viral code payload module.

However, Cass discloses the selected computer virus is formed of a detection module (section "Under the Skin", paragraph 10, lines 6-7), an infection module (section "Under the Skin", paragraph 6, lines 1-3), and a viral code payload module (section "Under the Skin", paragraph 8, lines 3-6).

It would have been obvious for one of the skill in the art to modify the White reference with the method taught by Cass to provide an effective defense by understanding the cause and mechanism of infection (Cass, page 56, paragraph 5, lines 1-3).

11. With regard to claims 3 and 12, White discloses a method and a computer readable medium wherein the detection module identifies a selected one of the client devices as a target client device (section "Cure Distribution", page 13, first paragraph, lines 1-2, update is returned to the client that reported the initial infection or other devices in the system)

12. With regard to claims 4 and 13, White discloses a method and a computer readable medium wherein those infected target client devices (section "Virus Detection", page 11, second paragraph, lines 1-2) but White does not disclose the infection module causes the virus to infect those target client devices not infected by the selected virus.

However, Cass discloses the infection module causes the virus to infect (section "Under the skin", page 57, paragraph 6, lines 1-3, invaded Word's default template reads on virus to infect) those target client devices not infected by the selected virus (section "Under the skin", page 58, paragraph 10, lines 2-4).

It would have been obvious for one of the skill in the art to modify the White reference with the method taught by Cass to provide an effective defense by understanding the cause and mechanism of infection (Cass, page 56, paragraph 5, lines 1-3).

13. With regard to claims 5 and 14, White discloses a method and a computer readable medium for virus analysis (abstract) but does not disclose the viral code payload module includes viral code that infects the targeted client device.

However, Cass discloses the viral code payload module includes viral code that infects the targeted client device (section "Source of Mischief", page 59, last section with component "Payload", section "Under the skin", page 58, paragraph 8, lines 3-6).

It would have been obvious for one of the skill in the art to modify the White reference with the method taught by Cass to provide an effective defense by

understanding the cause and mechanism of infection (Cass, page 56, paragraph 5, lines 1-3).

14. With regard to claims 6 and 15, White discloses a method and a computer readable medium for an anti-virus module (Fig. 3, page 14 and associated text; Section "Cure Distribution", page 13, paragraph 1, line 1, virus definition update reads on an anti-virus module).

White does not disclose modifying the infection module so that it introduces an virus infection into those client devices already infected by the selected virus.

However, Cass discloses the modifying the infection module (section "Under the Skin, page 57, paragraph 7, lines 1-4, "triggering Melissa which copied itself..." reads on modifying the infection module) so that it introduces an virus infection into those client devices already infected by the selected virus (section "Evolution of a sickness", page 56, paragraph 4, lines 6-8).

It would have been obvious for one of the skill in the art to modify the White reference with the method taught by Cass to provide an effective defense by understanding the cause and mechanism of infection (Cass, page 56, paragraph 5, lines 1-3).

15. Claims 7-9, and 16-18 are rejected under 35 USC 103(a) as being unpatentable over White, in view of Cass, and further in view of Maher, III et al. (US. Pat. No. 6910134), hereafter "Maher".

16. With regard to claims 7 and 16, White discloses a method and a computer readable medium for virus analysis (abstract) but neither White nor Cass discloses a incorporating inoculation viral code in the payload module that acts to prevent further infection by the selected virus.

Maher, on the other hand disclose incorporating inoculation viral code in the payload module (col. 10, lines 52-55, modifying bits of data packets reads on inoculation viral code in the payload module) that acts to prevent further infection by the selected virus (col. 10, lines 65-67).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to combine the teachings of White, Cass and teaching of Maher to scan network traffic at wire speeds, recognized emails potentially infected with viruses, and inoculate any attachment such that any virus in the attachment is destroyed (Maher, col. 1, lines 40-42).

17. With regard to claims 8 and 17, White discloses a repair viral code for the infected client device caused by the selected virus (section "Cure Distribution",

page 13, paragraph 1, virus definition reads on repair viral code, and update returned to client that reported the initial infection reads on infected client) but does not disclose the payload module.

On the other hand, Cass discloses a payload module (section "Under the skin", page 58, paragraph 8, lines 3-6).

It would have been obvious for one of the skill in the art to modify the White reference with the method taught by Cass to provide an effective defense by understanding the cause and mechanism of infection (Cass, page 56, paragraph 5, lines 1-3).

However, neither White nor Cass discloses incorporating repair viral code in the payload module that acts to repair any damage in the infected client device caused by the selected virus.

Maher, however, discloses incorporating repair viral code in the payload module (col. 10, lines 52-53, changing bits in the data packets reads on incorporating repair viral code in the payload) that acts to repair any damage in the infected client device caused by the selected virus (col. 10, lines 65-67, attachment will be unreadable reads on repair any damage in the infected client).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to combine the teachings of White, Cass and teaching of Maher to scan network traffic at wire speeds, recognized emails potentially infected with viruses, and inoculate any attachment such that any virus in the attachment is destroyed (Maher, col. 1, lines 40-42).

18. With regard to claims 9 and 18, White discloses a method and a computer readable medium for forming the anti-viral agent (section "Immune System Architectural Overview", page 10, paragraph one, lines 3-4) but does not disclose by combining the detection module, the modified infection module and the modified viral payload module.

Cass, on the other hand, discloses combining the detection module (section "Source of Mischief", page 59, second section, component "check whether computer is already infected by Mellisa", reads on detection module), the modified infection module (section "Under the Skin, page 57, paragraph 7, lines 1-4, "triggering Melissa which copied itself..." reads on modifying the infection module), and the viral payload module (section "Source of Mischief", page 59, third section, component "Payload").

It would have been obvious for one of the skill in the art to modify the White reference with the method taught by Cass to provide an effective defense by

understanding the cause and mechanism of infection (Cass, page 56, paragraph 5, lines 1-3).

However, neither White nor Cass discloses the modified viral payload module. On the other hand, Maher discloses the modified payload module (col. 10, lines 52-57, changing the bits of an attachment to render the attachment harmless reads on modified payload).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to combine the teachings of White, Cass and teaching of Maher to scan network traffic at wire speeds, recognized emails potentially infected with viruses, and inoculate any attachment such that any virus in the attachment is destroyed (Maher, col. 1, lines 40-42).

Conclusion

19. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. US. Pat. No. 5485575 to Chess et al. (Discloses extracting, sampling, and analyzing how computer virus attaches to a host program.)

b. US. PGPub. No. 2004/0148281 to Bates et al. (Discloses virus checking database which use part of virus status information as searching criteria).

c. US. Pat. No. 5832208 to Chen et al. (Discloses agent for detecting and removing e-mail attachment that infected with virus).

d. Vesselin Bontchev,, Are "Good" Computer Viruses Still a Bad Ideas?, Proceeding EICAR 1994 Conference, Pages: 25-47.

e. Stephanie Forrest et al., "Computer Immunology", Communications of the ACM, October 1997, Vol. 40. No. 10. pages: 88-96.

20. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

21. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Khoi Nguyen whose telephone number is 570-270-1251. The examiner can normally be reached on Mon-Fri (8:30 am – 5:00 pm est) If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor,

Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

22. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Khoi Nguyen
Art Unit 2132
Date: 7/16/07

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100